Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

COMMENTS OF TWILIO INC.

Twilio Inc.[1] ("Twilio") is pleased to submit these comments in response to the Federal Communication Commission's ("FCC" or "Commission") Further Notice of Proposed Rulemaking[2] ("FNPRM") seeking comment on proposed requirements to address foreign-originated illegal robocalls. Twilio strongly supports and has been an active participant in Commission and industry efforts to stop unlawful robocalls and restore trust in the public network. The implementation of STIR/SHAKEN and industry joint efforts to combat illegal robocalls, along with the Commission's increased scrutiny of international gateway providers, are productive steps toward combating illegal robocalls. But STIR/SHAKEN is not a silver bullet, and Twilio's own traceback efforts show that fraudulent calls often originate from bad

[1] Twilio Inc. offers cloud communications services that enable software developers to build, scale and operate real-time customer engagement, including voice, text, chat, email, and video, into web and mobile applications. Since its founding in 2008, Twilio has grown to a company of more than 7,000 employees, powering communications in more than 180 countries across Europe, Asia, and Latin America, in addition to the United States. Twilio powers more than 1 trillion annualized interactions every year and helps more than 250,000 customers—from small businesses to the world's largest multinational companies, from industries including education, healthcare, manufacturing, public safety, financial services, and many more—reinvent how they engage with their customers or constituents.

[2] *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59 & WC Docket No. 17-97, Fifth Further Notice of Proposed Rulemaking and Fourth Further Notice of Proposed Rulemaking, FCC 21-105 (2021) (*Gateway Provider FNPRM*).

actors overseas. These bad actors will continue to seek ways to access the U.S. network for as long as doing so is profitable. Twilio therefore welcomes this opportunity to comment on the Commissions' proposals to help prevent unscrupulous actors from reaching U.S. consumers.

I. GATEWAY PROVIDERS GENERALLY SHOULD BE SUBJECT TO THE SAME OBLIGATIONS AS OTHER VOICE SERVICE PROVIDERS AND INTERMEDIATE PROVIDERS

Given that foreign-originated illegal robocalls make up a significant portion of the illegal robocalls terminated to U.S. customers, Twilio supports the Commission's proposal to categorize certain providers as "gateway providers."[3] Given, however, that gateway providers may, like other providers, serve as a terminating voice service provider or an intermediate provider on a call-by-call basis, the Commission should define "gateway provider" as "the first U.S.-based provider in the call path for a foreign-originated call." This definition will capture gateway providers that transmit a call directly to another intermediate provider in the United States, as well as gateway providers that themselves terminate a call.[4]

Twilio believes that if a gateway provider is providing voice termination services to end-user customers in the United States, that gateway provider already is a voice service provider subject to the Commission's Caller ID Authentication rules, including the obligation to make appropriate certifications in the Robocall Mitigation Database.[5] Twilio therefore focuses its comments in this section on gateway providers acting as intermediate providers. As discussed in

[3] *See Gateway Provider FNPRM* ¶ 33.

[4] *Id*.

[5] 47 CFR 64.6300(l); 47 CFR 64.6305(b). As the Commission states, "[t]o the extent a gateway provider terminates a call in the U.S., it is acting as a terminating voice service provider and is already subject to our existing caller ID authentication and/or robocall mitigation rules." *See Gateway Provider FNPRM* ¶ 33 n100. If the Commission believes there is uncertainty on this point, Twilio urges the Commission to use this proceeding to provide clarity.

greater detail below, gateway providers should generally be subject to the same obligations as other voice service providers and intermediate providers (as appropriate).

A. All Gateway Providers Should Submit Appropriate Information to the Robocall Mitigation Database

Twilio agrees that intermediate providers, including gateway providers, must certify in the Robocall Mitigation Database (RMD) that they have implemented a robocall mitigation program or implemented STIR/SHAKEN technology.[6] This is consistent with the Commission's proposal to require gateway provides to submit a certification to the RMD that would include the "status of STIR/SHAKEN implementation and robocall mitigation on their networks; . . . contact information for a person responsible for addressing robocall mitigation-related issues; and [would] describe in detail their robocall mitigation practice."[7] Requiring all intermediate providers to submit certifications to the RMD will ensure that the Commission and industry alike have full visibility into the universe of providers that are responsible for fighting illegal robocalls and allow parties to evaluate the sufficiency of the robocall mitigation plans that each of those providers has described.

Given the differing roles of voice service providers and intermediate providers, Twilio suggests that the Commission provide clarity regarding appropriate robocall mitigation measures for intermediate providers, including gateway providers.

1. Gateway Providers Should "Know Their Customers"

It is likely that in many cases a gateway provider will not be able to "confirm that a foreign call originator is authorized to use a particular U.S. number that purports to originate the

[6] Letter from Joshua M. Bercu, USTelecom, to Marlene H. Dortch, FCC, WC Docket No. 17-97 at 4 (filed Sept. 18, 2020).

[7] *See Gateway Provider FNPRM* ¶ 94. However, Twilio does not have a stated preference as to whether the Commission should include additional information in its Robocall Mitigation Database requirements. *See id*. at ¶ 100.

call" because the provider that is delivering the call will, itself, be an intermediate provider.[8] Twilio therefore suggests that the "customer" that the gateway provider must "know" is the immediate upstream provider.[9] Gateway providers should conduct reasonable due diligence to ensure that the upstream providers that deliver traffic to them are legitimate, authorized service providers.

2. Gateway Providers Should Include Anti-Robocalling Clauses in their Customer Contracts

Twilio has established operational, technical, and contractual safeguards to prevent the placing of unlawful or unwanted calls through its platform.[10] Given how effective these measures are at preventing unwanted calls, Twilio believes that it is reasonable for gateway providers to "adopt specific contractual provisions addressing robocall mitigation with foreign providers from which the gateway provider directly receives traffic carrying U.S. NANP numbers, and, in some cases, traffic from their foreign-end user customers."[11]

B. GATEWAY PROVIDERS SHOULD MEET INDUSTRY STANDARDS FOR TRACEBACKS

As the Commission notes, "time is of the essence" when it comes to tracebacks where the Commission or law enforcement need to work with international regulators outside of U.S.

---

[8] *Id*. at ¶ 80.

[9] *See id*. at ¶¶ 84-85.

[10] Twilio has invested significant resources to support and reinforce the Commission and industry efforts to stop unlawful robocalls and restore trust in the public network. For example, Twilio implemented STIR/SHAKEN throughout its IP network ahead of the FCC's imposed deadline, currently serves on the Board of Directors of the Alliance for Telecommunications Industry Solutions ("ATIS"), is an executive committee member of USTelecom's Industry Traceback Group ("ITG") and is a member of the North American Numbering Council. Twilio also has implemented know-your-customer policies that satisfy the Anti-Robocall Principles adopted by State Attorneys General. *See Anti-Robocall Principles* (2019), https://www.ustelecom.org/wp-content/uploads/2019/08/State-AGs-Providers-AntiRobocall-Principles-With-Signatories.pdf.

[11] *See Gateway Provider FNPRM* ¶ 87.

jurisdiction.[12] Twilio itself has developed procedures to resolve traceback requests within 24 hours, and gateway providers should be expected to implement the provider traceback best practices adopted by the Industry Traceback Group, including that "[e]ach Voice Service Provider should endeavor to initiate investigation of the source of Suspicious Traffic request within four (4) business hours of receiving a request and strive to complete the investigation and return results within 24 hours."[13]

II. THE COMMISSION SHOULD ENCOURAGE IP INTERCONNECTION

For any given call, the full benefits of the STIR/SHAKEN authentication framework can be realized only if every carrier in the call path is capable of passing the authenticated caller identification information it receives (or originates) on to the next carrier in the call path. Some providers maintain both IP and non-IP portions of their networks but are currently choosing to interconnect with other providers on a non-IP basis. Calls that are properly originated within the STIR/SHAKEN framework that transit non-IP interconnection points arrive at their destination without authenticated caller identification information, frustrating industry and Commission anti-robocalling efforts. Twilio recognizes that there may be valid reasons for a provider to maintain non-IP interconnection with another carrier in some circumstances, but urges the Commission to provide incentives for all providers – including gateway providers – to interconnect on an IP-to-IP basis. Further, the Commission should consider how to encourage non-IP providers to implement STIR/SHAKEN in light of ATIS's adoption of a standard for out-of-band PASSporT transmission involving TDM networks.[14]

---

[12] *Id*. at ¶ 52.

[13] Industry Traceback Group, Policies and Procedures, at Appendix A, page 15 (July 2021), https://tracebacks.org/wp-content/uploads/2021/08/ITG_Policies-and-Procedures_2021.pdf.

[14] *See* Alliance for Telecommunications Industry Solutions, Signature-based Handling of Asserted information using toKENs (SHAKEN): Out-of-Band PASSporT Transmission Involving TDM Networks,

III. THE COMMISSION SHOULD CLEARLY DEFINE REASONABLE ANALYTICS FOR CALL BLOCKING AND ENSURE SUITABLE PROTECTIONS FOR LAWFUL CALLS

The FCC proposes to require gateway providers "to block calls that are highly likely to be illegal based on reasonable analytics."[15] As a general matter, Twilio supports the ability of carriers to block calls that are highly likely to be illegal or unwanted. However, Twilio continues to be concerned that inconsistent and non-transparent analytics may result in mislabeled critical, lawful calls.[16] All participants in the ecosystem would benefit from a better understanding of what constitutes "reasonable analytics," and if the Commission moves from permissive to mandatory call blocking in the case of gateway providers, it must take this opportunity to define reasonable analytics with more specificity.[17] Therefore, the Commission would benefit from gathering additional metrics on how to improve reasonable analytics.[18] Twilio notes that in the long-term, the criteria of whether or not to block a call could be based on whether the call has a validated SHAKEN token, but this will require full participation in the STIR/SHAKEN framework.

ATIS-1000096 (approved July 15, 2021), https://access.atis.org/apps/group_public/download.php/60535/ATIS-1000096.pdf.

[15] *See Gateway Provider FNPRM* ¶ 66.

[16] Comments of Twilio Inc., WC Docket No. 17-97, WC Docket No. 20-67, at 9-10 (filed May 15, 2020).

[17] *See Gateway Provider FNPRM* ¶ 70.

[18] *See generally Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, Declaratory Ruling and Third Notice of Proposed Rulemaking, 34 FCC 4876, 4888, para. 35 (2019) (providing examples for what combination of factors could be used in a calling blocking program, including large bursts of calls in a short timeframe; low average call duration; low call completion ratios; invalid numbers placing a large volume of calls; common Caller ID Name values across voice service providers; a large volume of complaints related to a suspect line; sequential dialing patterns; neighbor spoofing patterns; patterns that indicate TCPA or other contract violations; correlation of network data with data from regulators, consumers, and other carriers; and comparison of dialed numbers to the National Do Not Call Registry).

To the extent gateway providers engage in call blocking, they should be subject to transparency and redress requirements.[19] Specifically, Twilio supports the ongoing efforts of USTelecom's Blocking and Labeling Working Group and its "Best Practices Relating to Redress,"[20] and urges the Commission to consider the working group's progress before adopting rules applying specific transparency and redress requirements to providers, gateway or not.[21]

Respectfully submitted,

/s/ Rebecca Murphy Thompson

Rebecca Murphy Thompson
Head, North American Communications
Regulatory Affairs and Policy
Twilio Inc.
101 Spear Street
San Francisco, CA 94105

December 10, 2021

[19] *See Gateway Provider FNPRM* ¶ 75.

[20] *See* USTelecom Blocking and Labeling Working Group, *Best Practices Relating to Redress Requests* (2021), https://ustelecom.org/wp-content/uploads/2021/08/USTelecom-Blocking-and-Labeling-WG-Best-Practices-Relating-to-Redress-Requests-8-18-21.pdf.

[21] *See Gateway Provider FNPRM* ¶ 75; *see also* 47 CFR § 64.1200 (k)(8)-(10).